REMARKS / ARGUMENTS

In the Office Action dated July 8, 2011, the Examiner rejected all pending claims. In response to the Office Action, the Examiner's claim rejections have been considered. Applicant respectfully traverses all rejections regarding all pending claims and earnestly solicits allowance of these claims.

1. Claim Rejections - 35 U.S.C. §103

The Examiner rejected all pending claims under 35 U.S.C. §103 (a). Specifically, the Examiner rejected claim 1 as being unpatentable over Bush in view of Shefi.

Applicant submits that claim 1 is patentable over the cited references whether considered independently or in combination by at least reciting:

> A method for encrypting a digital data stream comprising the following steps:
> providing a communication device which has an interface for a digital storage medium, whose content may be read out and duplicated;
> providing the digital storage medium which is connected to the interface;
> storing a supply of symbols for encryption on the digital storage medium;
> providing a first random generator on the communication device which determines addresses on the digital storage medium;
> reading out the symbols from the digital storage medium using the addresses on the digital storage medium;
> employing the read out symbols for encrypting or decrypting the digital data stream of the communication device; and
> transmitting a status of the first random generator to synchronize the encryption or the decryption.

Support for the added limitation is found in original claim 13 as well as paragraph 17 of the applications as filed.

First, Bush fails to disclose "providing a first random generator on the communication device which determines addresses on the digital storage medium".

The Examiner argues that a person having ordinary skill in the art would have readily recognized the desirability and advantages of modifying the teachings of Bush with the teachings of Shefi by randomly determining an address of symbols on a storage medium. Furthermore, it is obvious that the teachings of Shefi would have improved the teachings of Bush by randomizing which symbols are selected for encryption by randomly generating addresses in order to provide

for secure communication using a one-time pad while protecting against brute force attacks on the one-time pad.

Applicant respectfully disagrees. The person of ordinary skill in the art would recognize that the teaching of Shefi is incompatible with Bush. In the encryption system of Bush it is impossible to randomly determine an address of symbols used for encryption because the one-time pad used for encryption in Bush is based on a specific structure which is need for the suggested encryption approach and would not be changed by the person of ordinary skill.

In detail, the contents of a sheet within a one-time pad in accordance with the teaching of Bush is illustrated in Fig. 2 and explained in paragraphs [0026-0027]:

> [0026] … Each sheet 104 contains a string 202 of N pure randomly-ordered numbers in the range of 1 to N. Each sheet 104 also contains a plurality of corresponding arrays 204. Number string 202 is a non-repeating sequence of numbers within the predetermined range N corresponding to the number of characters or positions in the encrypted data packet. For example, if the encrypted data packet will have five hundred positions, the numerals 1 through 500 will be randomly ordered and placed in string 202. Individual numbers within string 202 are employed to identify the position for a corresponding byte of data in the encrypted data packet. For example, the first number 206 within string 202 designates the position within the encrypted data packet in which the first byte of source data will be placed after encryption.
>
> [0027] Each individual number within string 202 has an associated array within array set 204. Each array 208 contains a non-repeating sequence of random numbers comprising a character map to be employed for the character in the respective position. For the sake of simplicity and clarity of explanation, the exemplary embodiment depicts only the mapping for numeric characters 0-9 and a delimiter ("*"). However, the mapping may easily be extended to include alphabetic or text characters merely by increasing the size of arrays 204. The arrays 204 essentially comprise encryption instructions for data packets not exceeding the length of position string 202.

This particular arrangement of numbers in the sheets of the one-time pad is necessary for the encryption algorithm shown in Fig. 4 and illustrated in Fig. 3. This algorithm determines a position indicator for each source plaintext character (from a source data packet of size N) in an encrypted data packet, the position indicator derived from string 202, thus implying that number string 202 is a non-repeating sequence of numbers within the predetermined range N. Next, the source character is replaced using a position dependent character map, defined by the

corresponding array 208. The necessary restrictions of the numbers in the array set 204 are explained in paragraph [0027] of Bush (see above).

Hence, the encryption algorithm in Bush necessarily depends on a one-time pad having random numbers which comply with a particular format and given restrictions. In other words, the one-time pad in Bush is not a simple sequence of true random numbers.

Shefi on the other hand teaches a method to generate a one-time pad by selecting true random numbers from a table of true random numbers according to a selection procedure (col. 10, lines 13-17). These selected numbers are true random numbers which do not comply with any restrictions (i.e. are stochastically random, see col. 9, lines22-24) such as the requirements for each sheet in the one-time pad of Bush.

Thus, the person of ordinary skill recognizes that randomly generated addresses to access random symbols on a storage medium cannot be used to improve the teachings of Bush and the teachings of Shefi cannot be directly applied to Bush.

Second, Bush and Shefi fail to disclose "wherein a status of the first random generator is transmitted to synchronize encryption and decryption".

The Examiner argues that the ordinarily-skilled person would have readily recognized the desirability and advantages of modifying the teachings of Bush in view of Shefi with the teachings of Kauffman by transmitting the status of a generator for synchronization. Kauffman recites motivation by disclosing that the receiver must have the same random number sequence the sender used or must be able to reproduce it in order to perform successful encryption and decryption.

Applicant respectfully disagrees. According to the claimed subject-matter, the first random generator on the communication device determines addresses on the digital storage medium which are used to read symbols for encryption. In order to synchronize the address generation for encryption and decryption, the status of the first random generator is transmitted.

Kauffman, on the other hand, discloses:

> [0031] … The RCPU accesses a multiplier and/or seed number from the receiver's one-time pad 210, via link 14, so that the receiver's PRNG 220 will generate and return a shift key via link 15. In one embodiment, the sender's one-time pads 150 and the receiver's one-time pad 210 are synchronized by other secret means conventionally known in the art, such that the outputs of the sender's PRNG 150 and receiver's PRNG 220 will enable the SCPU 100 and RCPU 200 to generate

> the same shift key. The same shift key used to encrypt the cryptogram and generated by the RCPU 200 is then sent to the receiver's shift cipher 230, via link 16.

Thus, Kauffman teaches that the pseudorandom generators PRNG in the sender and the receiver use the same multiplier and/or seed to generate the same shift key for encryption (see also [0027, 0029]). In order to maintain confidentiality of the transmitted data and avoid interception, it is absolutely necessary to use secret means for the synchronization. Any third party having knowledge of multiplier and/or seed could decipher the encrypted message.

The ordinarily-skilled person would therefore not be motivated by the teaching of Kauffman to modify the teachings of Bush in view of Shefi with the teachings of Kauffman by transmitting the status of a generator for synchronization. First, Kauffman does not suggest to synchronize the generation of addresses for reading random symbols by transmitting the status of a random generator, but suggests synchronization of pseudorandom generators for generation of shift keys for direct encryption/decryption. Next, Kaufman emphasizes that this synchronization requires other secret means, i.e. another secure channel between sender and receiver. This would further discourage the ordinarily-skilled person from applying the teaching of Kauffman to Bush in view of Shefi.

In summary, not even the combination of three documents (which the skilled person would have no motivation to combine) would have lead the skilled person to the claimed invention which therefore is not obvious. Therefore, claim 1 is patentable over the cited references.

As claim 13 recites limitations similar to claim 1, Applicant request withdrawal of the rejection of claim 13 for the same reasons cited above.

The remaining claims are patentable by virtue of their dependency and for reciting additional limitations.

CONCLUSION

Applicant has made an earnest and *bona fide* effort to clarify the issues before the Examiner and to place this case in condition for allowance. Reconsideration and allowance of all of claims is believed to be in order, and a timely Notice of Allowance to this effect is respectfully requested.

The Commissioner is hereby authorized to charge any additional required fees from Deposit Account No. 50-2586, Deposit Account Name PERKINS COIE LLP.

Should the Examiner have any questions concerning the foregoing, the Examiner is invited to telephone the undersigned attorney at +1.206.359.3535.

Respectfully submitted,

Date: January 4, 2012

/Aaron Wininger, Reg. No. 45,229/

Aaron Wininger
Reg. No. 45,229
PERKINS COIE LLP
1201 Third Avenue
Suite 4800
Seattle, WA 98101-3099